Certified Information Systems Security Professional (CISSP)

Course Outline

Certified Information Systems Security Professional

Days of Training: **5**

Overview

An internationally respected certification, the CISSP continues to serve as the absolute pinnacle of information security training for knowledgeable and highly accomplished mid to senior level professionals in the IT industry. This 5-day course will expand upon your knowledge by addressing the essential elements of the eight domains that comprise a Common Body of Knowledge (CBK)® for information systems security professionals. The course offers a job-related approach to the security process, while providing a framework to prepare for CISSP certification. By defining eight security domains that comprise a CBK, industry standards for the information systems security professional have been established. The skills and knowledge you gain in this course will help you master the eight CISSP domains and ensure your credibility and success within the information systems security field.

Lesson 1: Security and Risk Management

- Security governance principles
- Compliance
- Professional ethics
- Security documentation
- Risk management
- Threat modeling
- Business continuity plan fundamentals
- Acquisition strategy and practice
- Personnel security policies
- Security awareness and training

Lesson 2: Asset Security

- Asset classification
- Privacy protection
- Asset retention
- Data security controls
- Secure data handling

Lesson 3: Security Engineering

- Security in the Engineering Lifecycle
- System component security
- Security models
- Controls and countermeasures in Enterprise Security
- Information system security capabilities
- Design and architecture vulnerability mitigation
- Vulnerability mitigation in embedded, mobile, and web-based systems
- Cryptography concepts
- Cryptography techniques
- Site and facility design for physical security
- Physical security implementation in sites and facilities

Lesson 4: Communications & Network Security

- Network protocol security
- Network components security
- Communication channel security
- Network attack mitigation

Lesson 5: Identity & Access Management

- Physical and logical access control
- Identification, authentication, and authorization
- Identity as a Service
- Authorization mechanisms
- Access Control Attack Mitigation

Lesson 6: Security Assessment & Testing

- System Security Control Testing
- Software Security Control Testing
- Security Process Data Collection
- Audits

Lesson 7: Security Operations

- Security operations concepts
- Physical security
- Personnel security
- Logging and monitoring
- Preventative measures
- Resources provisioning and protection
- Patch and vulnerability management
- Change management
- Incident response
- Investigations
- Disaster recovery planning
- Disaster recovery strategies
- Disaster recovery implementation

Lesson 8: Security in the Software Development Lifecycle

- Security Principles in the System Lifecycle
- Security Principles in the Software Development Lifecycle
- Database Security in Software Development
- Security Controls in the Development Environment
- Software Security Effectiveness Assessment

1 Maritime Square
#10-24/25 HarbourFront Centre
==========
Singapore 099253

New Horizons Singapore
Tel: +65 6822 8282 Fax: +65 6822 1282
Email: info@newhorizons.com.sg